Claims

1. Method for decrypting data, the data comprising a first and a second data set, the first and second data set being encrypted, wherein said first data set (AV_E) and a respective electronic decryption key (K3) are stored on a removable read-only storage medium (D), and the second data set (SD_E) is not stored on said removable read-only storage medium (D) but is related to the first data set (AV_E), **characterized in**
   - retrieving the first data set (AV_E) from the removable read-only storage medium (D);
   - retrieving the decryption key (K3) from the removable read-only storage medium (D);
   - retrieving the second data set (SD_E) from a second data source (IN);
   - decrypting said first data set (AV_E) using said decryption key (K3); and
   - decrypting said second data set (SD_E) using said decryption key (K3).

2. Method according to claim 1, wherein the first data set (AV) comprises at least audio-visual data, and the second data set (SD) is a supplementary data set.

3. Method according to claim 1 or 2, wherein the second data set (SD) comprises one or more of subtitle-, audio-, video- or graphics data, playlists, movie objects, executables, bonus tracks, games or screen savers.

4. Method according to any of the previous claims, wherein the electronic decryption key (K3) is only accessible while a removable read-only storage medium (D) that

contains said electronic decryption key (K3) is readable.

5. Method according to any of the previous claims, wherein two or more electronic decryption keys (K1,K2) are stored on the removable read-only storage medium, wherein at least one of said keys can be used for decryption of the first data set (AV_E) and another of said keys can be used for decryption of the second data set (SD_E).

6. Apparatus for decrypting a data set, the data set comprising a first and a second data set, the first and second data set being encrypted, wherein said first data set (AV_E) and a respective electronic decryption key (K3) are stored on a removable read-only storage medium (D), and the second data set (SD_E) is not stored on said removable read-only storage medium (D) but is related to the first data set (AV_E), **characterized in** that the apparatus comprises
- means for retrieving the first data set (AV_E) from the removable read-only storage medium (D);
- means for retrieving the decryption key (K3) from the removable read-only storage medium (D);
- means for retrieving the second data set (SD_E) from a second data source (IN);
- means for decrypting said first data set (AV_E) using said decryption key (K3); and
- means for decrypting said second data set (SD_E) using said decryption key (K3).

7. Apparatus according to claim 6, further comprising local storage means (HD) for storing said first or second data

set, or parts of said first or second data set, before decryption.

8. Method or apparatus according to any of the previous claims, wherein the electronic decryption key (K3) is the only suitable key for decrypting the first data set (AV_E), but is one of several suitable keys for decrypting the second data set (SD_E).

9. Method or apparatus according to any of the previous claims, wherein the removable read-only storage medium (D) is an optical disc.

10. Method or apparatus according to any of the previous claims, wherein the first and second data sets are encrypted using RSA (Rivest-Shamir-Adelman) coding.